In collaboration with Deloitte

WORLD ECONOMIC FORUM

Transitioning to a Quantum-Secure Economy

WHITE PAPER

SEPTEMBER 2022

Images: Getty, Unsplash

Contents

Foreword

Jeremy Jurgens
Managing Director,
World Economic Forum

Isaac Kohn
Partner, Deloitte,
Switzerland

Colin Soutar
Managing Director,
Deloitte, USA

Quantum technologies continue to fascinate and their applications have the potential to transform our lives. The quantum computing age is growing ever closer and it could render obsolete some of the encryption on which most enterprises, digital infrastructures and economies currently rely. Addressing this issue requires prompt action at the national and global levels.

Unlike Y2K, the impact of a corresponding "Y2Q" (year to quantum) is fairly well known, but the timeline is unpredictable. Further, there is a belief that data is being harvested now for decryption later once quantum computers are available. The uncertainty surrounding when quantum will be mainstream makes it hard to discern the right time to take action and tends to lead to de-prioritization in favour of more immediate issues.

Building an understanding among senior leaders of the risks and immediate steps required to ensure a secure quantum transition is therefore a critical priority identified by both the World Economic Forum's Global Future Council on Cybersecurity and the community engaged in the Future Series: Cyber 2025 initiative.

Over the past year the Forum, in collaboration with Deloitte, has worked with a community of senior executives and experts from business, academia, government and non-profit organizations to develop a deeper understanding of the emerging risks and to provide insights and guidance to ensure a secure transition to the quantum economy. We hope this report will help drive individual and collective action globally to address the key security challenges while realizing the transformative potential of quantum technologies.

Executive summary

To harness the potential opportunities opened by quantum computing, organizations need to act now on the quantum threat.

Quantum computing promises transformative simulation and modelling capabilities across a diverse range of industries. However, these advances in computational power will also introduce significant risks via the potential threat of disruption to some widely used encryption standards. While definitive timelines for both quantum computing applications and the associated quantum cybersecurity threats have not yet fully materialized, organizations must act now to evaluate their readiness to adapt to the quantum threat.

The quantum threat is expected to have a large and disruptive impact on the current digitally dependent economy. An orderly response is highly desirable over a reactive one. It is a business imperative that organizations start to think about what a secure quantum transition could look like and understand their cryptographic and data exposure to avoid disruption of business operations. The unknown timeline of this quantum risk – which could lead to a "not me, not now" response – may impose a more significant impact than is necessary.

This white paper arises from in-depth discussions between senior leaders and quantum experts from the quantum security working group, part of the quantum computing network of the World Economic Forum. The paper provides guidance for a secure quantum transition, which organizations need to embrace now to avoid playing catch-up with the technology. To achieve this transition, organizations need to:

- **Build awareness around the quantum threat,** by educating senior leaders on the systemic impact. The quantum threat feels far away and largely abstract for many organizations. To combat this, organizations will need to face what is known, but also accept there are implications that are still unknown. Conducting initial quantum readiness assessments will help leaders determine the specific threats their organizations face. Executive buy-in is key to ensure the quantum transition attracts appropriate investment and prioritization.

- **Plan and prepare by adopting a quantum-safe strategy and transition roadmap.** Addressing the quantum threat requires organizations to plan and create a timeline that sequences immediate, near-term (3-5 years) and longer-term actions. Organizations should consider adopting a "crypto-agile" posture, enabling them to readily transition cryptographic capability. This will help them prioritize a transition to quantum security as technology advancements and threat knowledge continue to evolve.

- **Initiate the transition, leveraging hybrid solutions.** Organizations adopting quantum-resistant security will more than likely leverage hybrid solutions that integrate both classical and quantum-ready approaches. This will give organizations some assurance that existing security remains intact, while overlaying that security with relatively new post-quantum cryptography algorithms.

Introduction

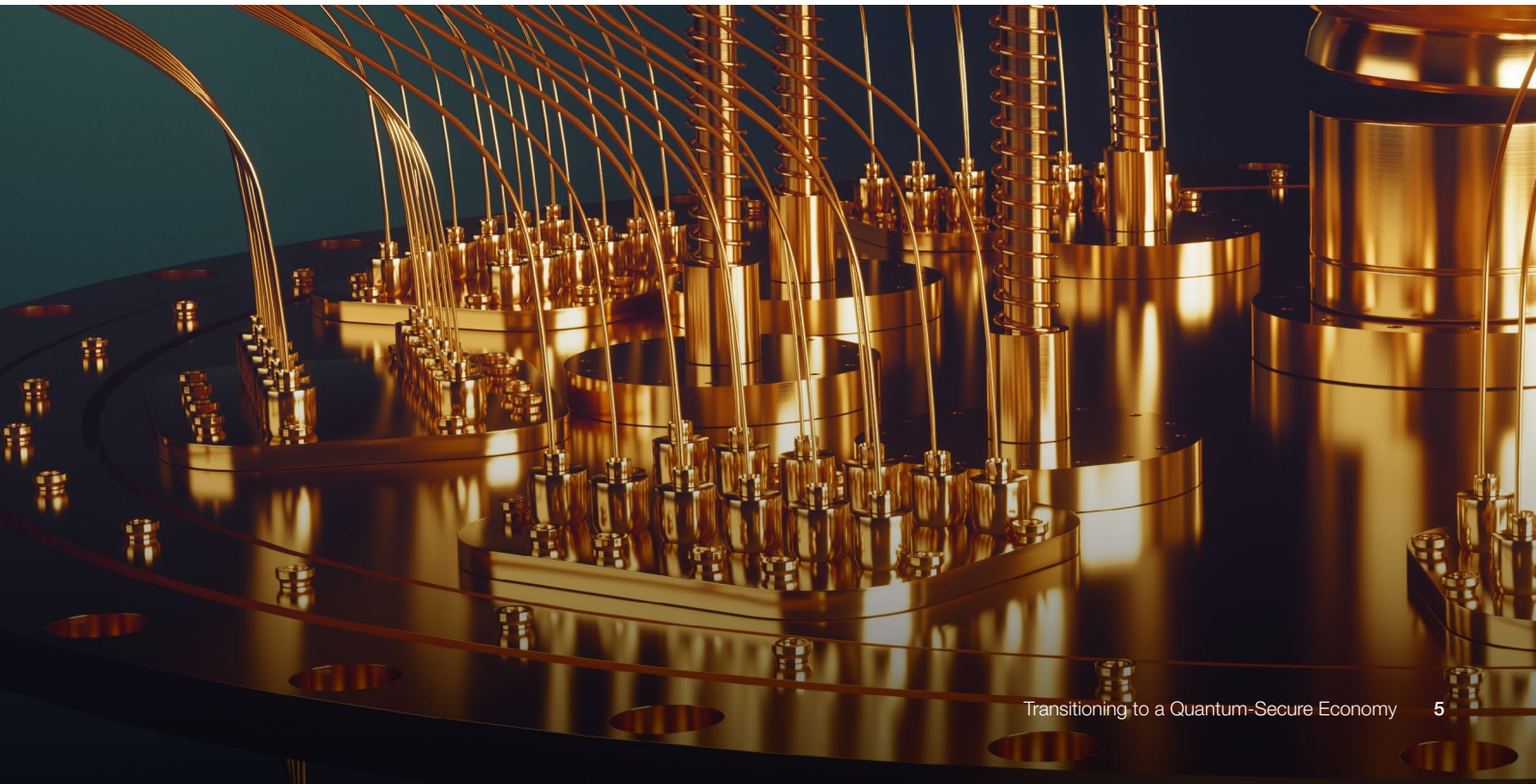
The establishment of governance principles is key to building trust in quantum and to pre-empt possible risks before the technology is commercialized.

Quantum computing has the potential to drive transformational changes across industry and society. The growing interest and investment in developing quantum computing by major technology corporations, national governments and venture capitalists highlight its importance. In 2021, the quantum computing market earned $490 million, with estimates of public funding surpassing $24 billion.[1] Private investments in quantum start-ups have skyrocketed to more than $1 billion.[2] The race to unlock the potential of quantum computing has the potential to drive trillions of dollars of value across the global economy during the coming years, with cybersecurity market spending forecast to grow $3 billion per year to reach $30 billion by 2030.[3] These investments will likely drive further developments around diverse quantum security solutions, such as post-quantum cryptography, quantum random number generation, quantum key distribution and quantum communication technologies.

The quantum computing age unlocks multiple optimization and simulation opportunities across industries, through its ability to solve specific mathematical problems in a significantly faster and more efficient manner than was previously possible. Some of the applications being considered include quantum machine learning, simulation of complex systems and modelling of material science. However, the arrival of quantum computing and its ability to speed up certain complex mathematical computations could render obsolete the current encryption on which most enterprises, digital infrastructures and economies rely. Quantum technologies therefore represent a significant and tangible risk to digital economies, with potential global impact. If this risk materializes, it could overshadow the great benefits that quantum technologies could offer mankind. It has even recently been referred to as the "Encryptogeddon".[4]

The timeline associated with the maturity of quantum computing is still uncertain, but recent advancements in the field have amplified the need to take near-term actions to prepare a secure transition to the quantum era. For example, the Canadian company Xanadu Quantum Technologies reported in June 2022 that Borealis, their quantum computer in the cloud, can perform a single task 50 million times faster than a classical computer, improving on the early results demonstrated by China's quantum computer in June 2021 and Google in 2019.[5] [6] [7]

"The significant risk to digital economies posed by quantum computing has led it to be dubbed "Encryptogeddon".



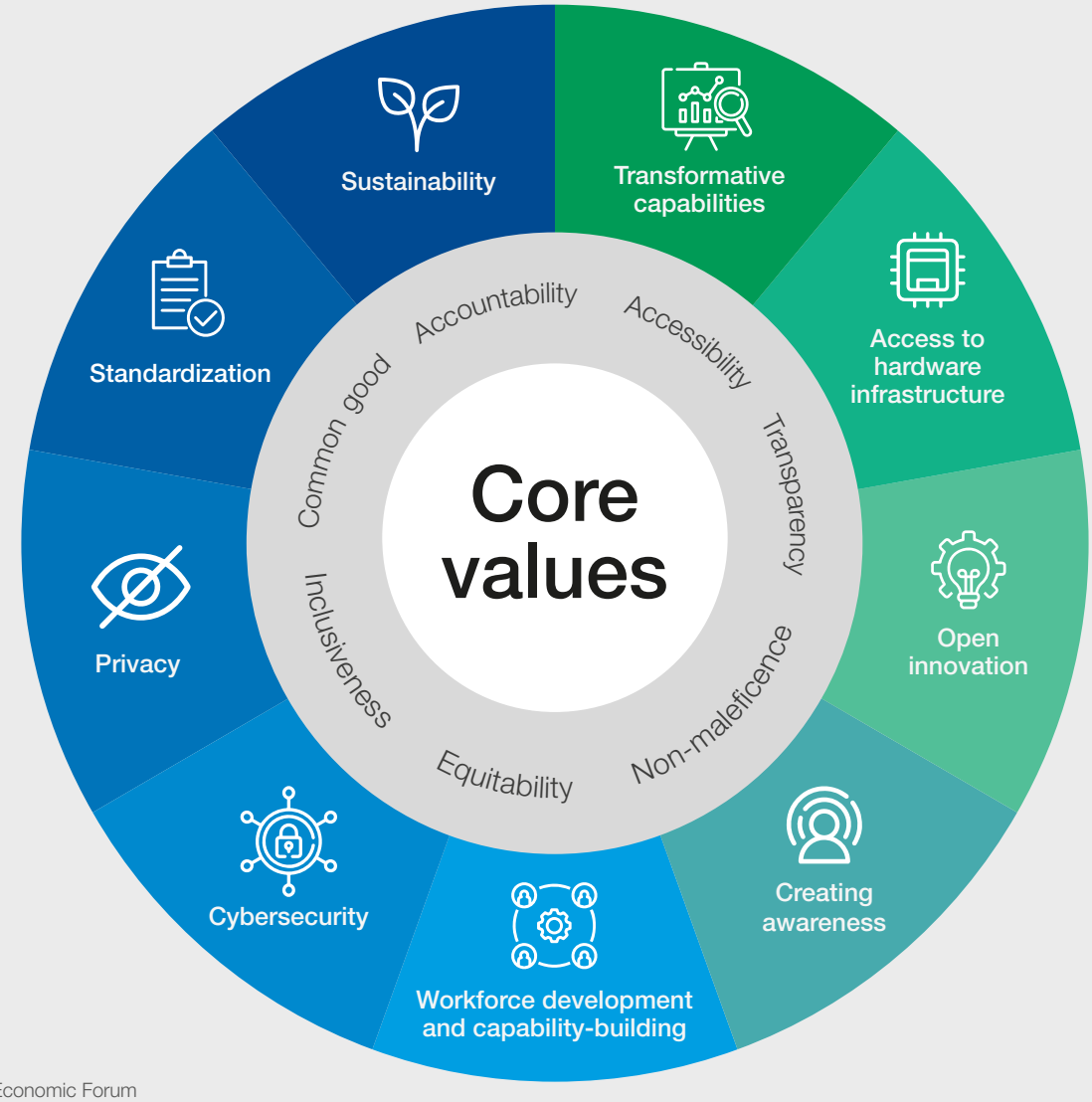
While the quantum risk is understood by some within the technical community and defensive solutions are being developed, further clarification of the significant challenges and impacts needs to be developed in a way that is digestible by senior leadership. Diverse global stakeholders, including governments, experts and larger communities of interest, have called for urgent action. In May 2022, US President Biden announced an executive order and memorandum to address the quantum threat by 2035.[8] [9] In July, the US's National Institute of Standards and Technology (NIST) announced a list of four quantum-resistant cryptographic algorithms, after thorough evaluation by the expert community. Yet while some organizations have already started the transition journey, others are still questioning the real benefits and challenges brought by the technology.

To ensure the responsible development and use of quantum computing, the governance working group of the World Economic Forum's quantum computing network has developed a set of governance principles, themes and core values (see Figure 1).[10] The proactive establishment of governance principles is key to building trust in the technology and to pre-empt possible risks before the technology is commercialized. Cybersecurity is one of the key principles for ensuring a safe transition while harnessing the transformative capabilities of quantum computing.

Developing a coherent approach for transitioning to a quantum-secure economy requires a broad, collaborative and critical approach from a diverse and global community of business and cybersecurity leaders. This white paper has been informed by a wide-ranging group of participants from across the Forum's quantum security community and Global Future Council for Cybersecurity.[11]

This paper seeks to help senior leaders, policy-makers, regulators, business executives and decision-makers in cybersecurity, strategy, innovation and risk management to understand the potential impact of quantum cyber risks and to take the necessary steps to ensure a secure transition.

FIGURE 1 **Quantum computing governance principles, themes and core values**



Source: World Economic Forum

This white paper **will**:

- Provide clarification on the impacts of the quantum threat
- Present steps and a consensus-based framework to help guide organizations throughout the transition towards a quantum-safe environment
- Develop guidance for senior business leaders, cyber leaders and policy-makers to manage the risks and secure the quantum transition
- Clearly articulate the characteristics of three emerging technologies that can help mitigate the quantum threat: post-quantum cryptography (PQC), quantum key distribution (QKD) and quantum random number generation (QRNG)
- Determine emerging focus areas for research and investment and enhance cybersecurity capabilities to counter future systemic risks

This white paper **will not**:

- Explore general quantum computing applications
- Focus on systemic risks that are not created or amplified by the quantum threat and quantum security solutions
- Provide detailed sectoral or geographical perspectives in relation to the exploration or mitigation of identified systemic risks
- Deliver in-depth technical explanations of quantum computing technologies or the cybersecurity dimensions of use cases
- Highlight specific products or solutions that can be used – instead we will use generic use-case descriptions

How to read this report

This report comprises six chapters that discuss the potential impact of quantum on security, as well as actions to take to ensure a secure transition towards a quantum economy:

Chapter 1: Why prioritize quantum security? Introduces quantum computing, the threats, opportunities and timeline.

Chapter 2: How to begin the quantum-safe transition? Discusses some of the independent timelines for key drivers and identifies actions that can be taken now.

Chapter 3: How to adopt a quantum risk management approach? Provides a global consensus-based framework to ensure action in the short-, medium- and long-term.

Chapter 4: What is required from different stakeholders? Offers guidance for various audiences to initiate the post-quantum transition.

Chapter 5: What technologies are available to address the quantum threat? Defines the current technology landscape and differentiates key technology approaches.

Chapter 6: What are the focus areas for future attention? Identifies future research, investment and governance needs and opportunities.

1 Why prioritize quantum security?

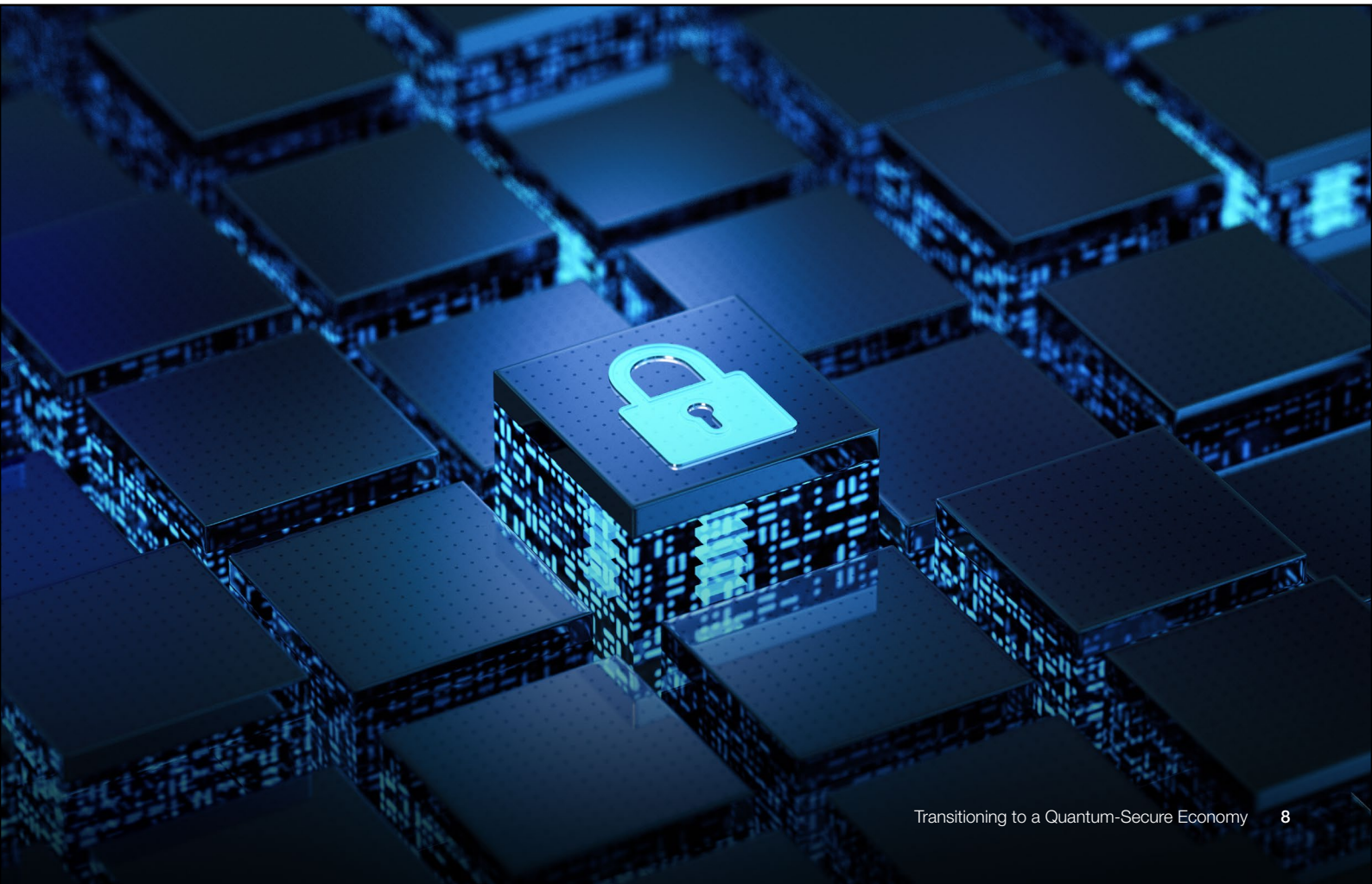
Quantum computing will enable great innovations in the future but will be accompanied by great risk.

Emerging technologies such as artificial intelligence (AI) and cloud computing consistently promise to address our most pressing problems, giving many a sense of both inspiration and scepticism. Quantum technologies are no exception. For many, the word “quantum” is more likely to conjure thoughts of science-fiction than one of today’s news headlines. Yet, what are quantum computers? When will the quantum threat become mainstream? And most importantly, what is the potential impact of the quantum threat?

Quantum mechanics, first conceived at the beginning of the 20th century, explains foundational concepts of how basic matter exists, changes and interacts over time. Those initial discoveries fascinated scientists for the next several decades and inspired ground-breaking innovations such as lasers and magnetic resonance imaging systems. Perhaps most notably, it enabled the invention of the semiconductor transistor, which is the cornerstone of the computer industry and is considered the highlight of the first quantum revolution.

More recently, a second quantum revolution has been underway, garnering attention for advanced applications such as quantum computing, quantum sensing and quantum communications. As opposed to the first quantum revolution where quantum properties were used to manufacture superior devices (lasers, transistors, etc.), the second quantum revolution refers to the storage and processing of information in quantum devices. This emerging field of quantum information science will have the capacity to drive high-impact use cases in the future. However, its transformative power is still limited due to the infancy of today’s quantum hardware.

“ Quantum mechanics enabled the invention of the semiconductor transistor, the cornerstone of the computing industry.



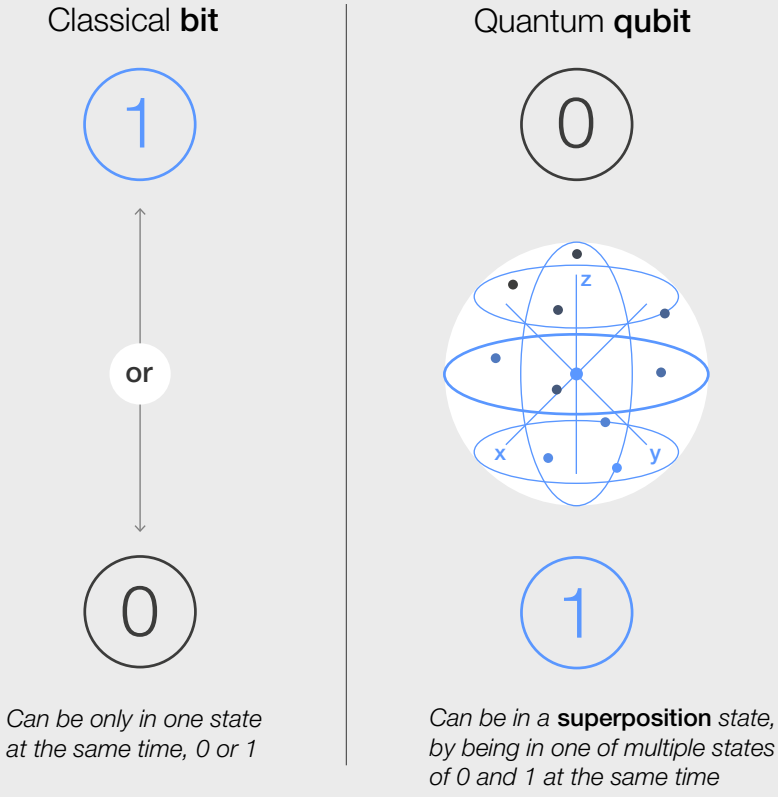
1.1 What are quantum computers?

Quantum computers are a new type of computing device capable of performing specific calculations, some of which are intractable with classical computers.

In classical computing, all information is represented in bits (as 0s and 1s). Quantum computers use qubits that combine 0s and 1s at the same time (called "superposition"). Leveraging the principles of superposition and entanglement (the ability of remote qubits to be correlated to each other), quantum computing enables a new way of storing and processing information. These new building blocks are used to construct quantum algorithms that, in some cases, significantly accelerate the ability to solve computational problems (see Figure 2).

There are already multiple quantum algorithms that show potential to achieve significant speed-up compared to classical algorithms. These include algorithms for solving combinatorial problems, simulation of physical systems, accelerating machine learning algorithms and more.

FIGURE 2 **Classical vs. Quantum computer**



1.2 When will the quantum-threat become mainstream?

Experts forecast the quantum threat will materialize in 10 years – but it could be sooner, given the secrecy of certain nations looking for strategic advantage.

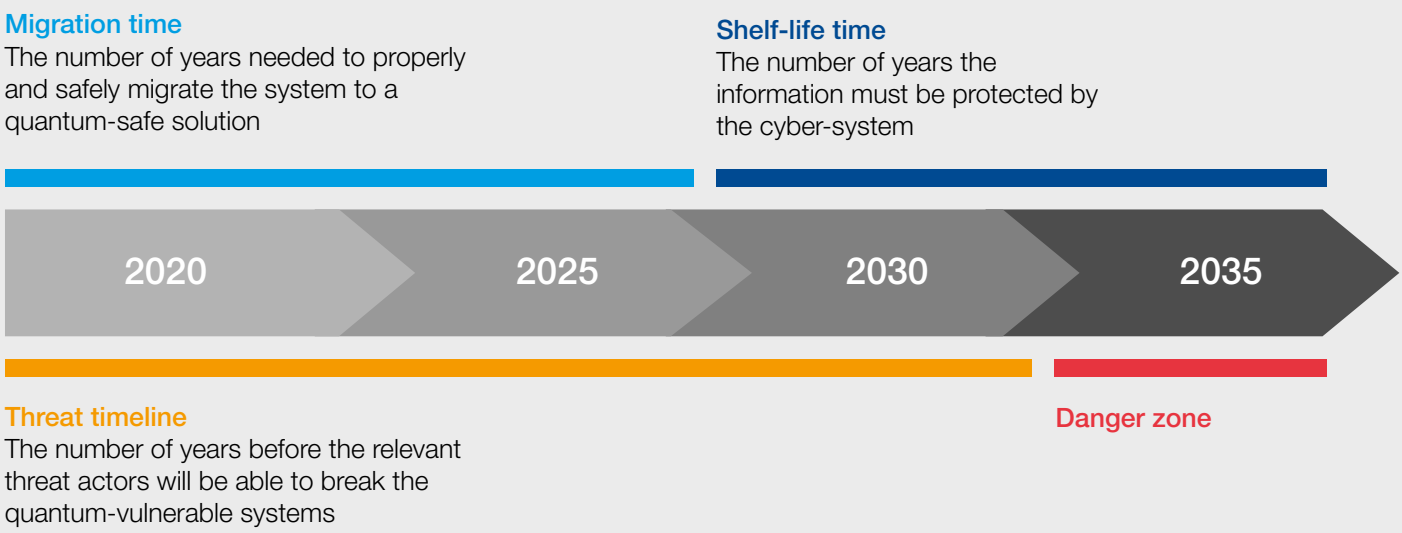
The field of quantum computing is still in its infancy and the machines we have today are still far from being mainstream and threatening cybersecurity. Leading experts in the field forecast the quantum threat will materialize in about 10 years.[12] This timeline, although uncertain, could arguably be even shorter – especially given the asymmetry of information and secrecy across the globe regarding the advancements in quantum computing by certain nations looking for strategic advantage.

Regardless of this timeline, organizations need to take a risk management approach and understand that the timeline is accelerating towards the "shelf-life" and "danger zone" (see Figure 3). With migrations of previous algorithms taking approximately 10 years, it is vital for organizations to pioneer the shift to quantum-safe cryptography to thrive and stay protected from cyberattacks.

The precise threat timeline you should focus on depends on your risk tolerance. For very critical systems and assets, the likelihood of quantum attacks in five years is becoming material and for most critical systems and assets I believe the 10-year likelihood needs to be addressed assertively.

Michele Mosca, University of Waterloo, Canada

FIGURE 3 **Quantum threat timeline**



Source: Michele Mosca, University of Waterloo, Canada[13]

1.3 What is the potential impact of the quantum threat?

The quantum cyber threat is likely to materialize within the lifecycles of many IT/OT systems being deployed today; the cyber risk, however, particularly for long-lived data, is clear and present today.

Vikram Sharma, Founder & CEO, QuintessenceLabs

When quantum computing gains traction, it will break some of the current cryptographic algorithms. A great deal of the security of our digital society relies on these cryptographic algorithms to guarantee the confidentiality (data privacy) and integrity (data accuracy) of our message exchanges, online banking operations and stored data in the cloud. Most of these algorithms' security builds on mathematical problems that are considered intractable on classical computers but that become solvable with quantum computers. This threatens the security of the cryptographic algorithms that are a fundamental part of our digital lives.

There are currently two algorithms – Shor and Grover – that quantum computers can use to break the hard mathematical problems that underpin some of our existing cryptography. Shor's algorithm can be used to break the factorization problem in a matter of hours or even minutes,[14] rendering public-key cryptographic algorithms useless.[15] Grover's algorithm can be used to speed up the search for the secret key used by symmetric cryptography to guarantee the confidentiality of most of our data exchanges and storages, as well as the search for the passwords we use to secure our personal accounts.[16]

The impact of the quantum threat does not stop with cryptographic algorithms, as its cascading effects can be potentially large. With infrastructure breakdowns being one of the main concerns for cyber leaders, this places it among the highest challenges business organizations face in the future.[17] The examples below illustrate some of the systemic risks around how the quantum threat could affect our daily lives:

$4.35m
Average cost per data breach

– **Increasing data breaches of sensitive health and financial personal data**. Data breaches are already one of the largest cyber challenges for organizations, with average costs per data breach reaching $4.35 million. Imagine if all your private and sensitive communications and information become public? Most information exchanges between organizations, individual citizens, and financial and governmental institutions are fully digital and rely on cryptographic systems to ensure they are kept private. Quantum computers provide the ability to intercept and decrypt this data. This will lead to large reputational impacts for organizations as well as impacts on the privacy of individuals, who could find their private sensitive information in the public domain.

– **Threatening internet and message exchanges.** In today's digital world, internet traffic and instant messaging are a fundamental part of our daily lives, with private and sensitive personal exchanges. These exchanges are protected by a secure communication channel that uses public-key encryption algorithms to exchange a unique key to secure the communication. Quantum computers could be used to break this secure channel and eavesdrop on practically every encrypted exchange. This makes all private and secret communications transparent to malicious users.

– **Challenging the integrity of digital documents.** In our increasingly digital society, there is a growing need to ensure the integrity and authenticity of data and information. As paper documents and identities become replaced by digital versions, this need becomes supremely important. Attacks using quantum computers could be used to challenge and forge the digital versions of information, identities and sensitive data.

– **Breaking cryptocurrencies.** As cryptocurrencies become more mainstream, they are increasingly a target for cyber attacks. This is because they are built with blockchain technology that relies heavily on cryptography algorithms for data integrity, transaction processing, proof of ownership and more. Quantum computing could pose a systemic risk to cryptocurrencies by breaking their underlying cryptography. Recent research has demonstrated that about 25% of bitcoins and 65% of ether coins could be vulnerable to a quantum attack. At current rates, this could represent more than $40 billion of value at risk.[18]

– **Risk of "harvest now, decrypt later" attacks.** For certain types of data (e.g. confidential and sensitive) that have both high data value and long shelf-life characteristics, the quantum threat might already be materializing today in the form of an attack known as "harvest now, decrypt later". Certain attackers may currently be intercepting encrypted data transmissions and storing them on a hard disk drive for later use. Although the encrypted data may not be of any value today, it could still be of interest 10 or 15 years from now when the attacker has access to a cryptographically relevant quantum computer. This is of particular concern for regulated industries that are required to keep sensitive customer data for long periods of time.

"About 25% of bitcoins and 65% of ether coins could be vulnerable to a quantum attack, putting more than $40 billion of value at risk.

2

How to begin the quantum-safe transition

Regardless of unpredictable timelines, organizations should think about their transition to quantum-safe cryptography now, as the process will take time.

20 billion digital devices will need to be upgraded or replaced with post-quantum cryptography in the next 20 years.

The World Economic Forum's Global Future Council on Quantum Computing estimates that 20 billion digital devices will need to be upgraded or replaced with post-quantum cryptography in the next 20 years.[19] This upgrade is not a simple switch-out or patch, because cryptography is entrenched across enterprises, often in physically remote systems. For example, migrating to post-quantum cryptography will affect the performance requirements of microprocessors that are embedded in ATM machines, TV set-top boxes, point-of-sale systems, smartphones and a host of other devices and systems. As a result, algorithm replacement can be extremely disruptive and take years to complete; typically, it requires upgrading or replacing components of the cryptographic infrastructure. This is one of the reasons organizations must start now to consider what their migration plan should be and assume a posture of crypto-agility that would allow them to quickly update.

2.1 What are the steps to consider?

Not all data generated today will still be relevant when the quantum threat materializes.

Build awareness of the quantum threat, by understanding the risk that quantum computing poses to existing cryptographic and encryption systems, as well as the macro impact to the organization's business model. This awareness will help to educate senior leaders from the public and private sectors, including boards, C-suites, government heads, policy-makers and operational-level executives, to gain broad support for investments in a quantum-safe cryptography infrastructure.

Plan and prepare for the quantum threat, by assessing the different areas of the digital and infrastructure environment to devise a prioritized action plan.

Understand the lifetime of data. As it is expected to take some years before quantum computers can break cryptography, not all data generated today will still be relevant when the quantum threat materializes. It is therefore important to classify the longevity of data in order to assess whether protection against the quantum threat is needed in the short term. For example, state secrets must be kept secret for a long time (even indefinitely), while the digital signature for a one-year contract is not likely to be relevant after the contract expires.

Take a fresh look at cryptographic governance. Preparing cryptographic systems for the quantum computing era is a major technological challenge. In the same way that agile software delivery practices helped create more adaptable technology organizations, so a more agile approach to cryptographic governance can create more flexible businesses and infrastructure that will quickly pivot and reprioritize in response to evolving security challenges and requirements.

Assess readiness for and work towards greater crypto-agility. A more crypto-agile organization is one that can efficiently update cryptographic algorithms, parameters, processes and technologies to better respond to new protocols, standards and security threats, including those leveraging quantum computing methods. To assess organizational readiness for crypto-agility, consider the following:

– *Data and cryptographic assets.* To help respond to systemic changes, such as new algorithms, organizations should provide an account of their data assets to understand how they are currently cryptographically protected. This means inventorying and prioritizing cryptographically protected data, transactions and other assets

to understand their retention requirements and locations (e.g. are they on-premises or in the cloud). It is important to note that inventorying cryptographic assets is initially a time-intensive process and requires updating as new technology and services are adopted.

– *Cryptographic keys.* To identify and prioritize future vulnerabilities, business leaders should review the types of cryptographic keys being used, their characteristics and their locations in existing computer and communications hardware, operating systems, application programs, communications protocols, key infrastructures and access control mechanisms.

– *Infrastructure limitations.* Quantum-safe cryptography may use substantially more processing power than current cryptographic methods, which in turn could require infrastructure upgrades. As NIST standards develop, it will be important to understand how they affect system infrastructure, identify potential future infrastructure shortcomings and develop a plan for addressing them.

Initiate the transition, leveraging hybrid solutions. Organizations adopting quantum-resistant security technologies will more than likely leverage hybrid approaches that integrate both classical and quantum-ready solutions. This will give organizations reassurance that existing security remains intact, while overlaying that security with relatively new post-quantum cryptography algorithms. Organizations should set their short-, mid- and long-term goals, review the different deployment scenarios, opportunities and challenges they may face, and fashion strategies that are fit for purpose.

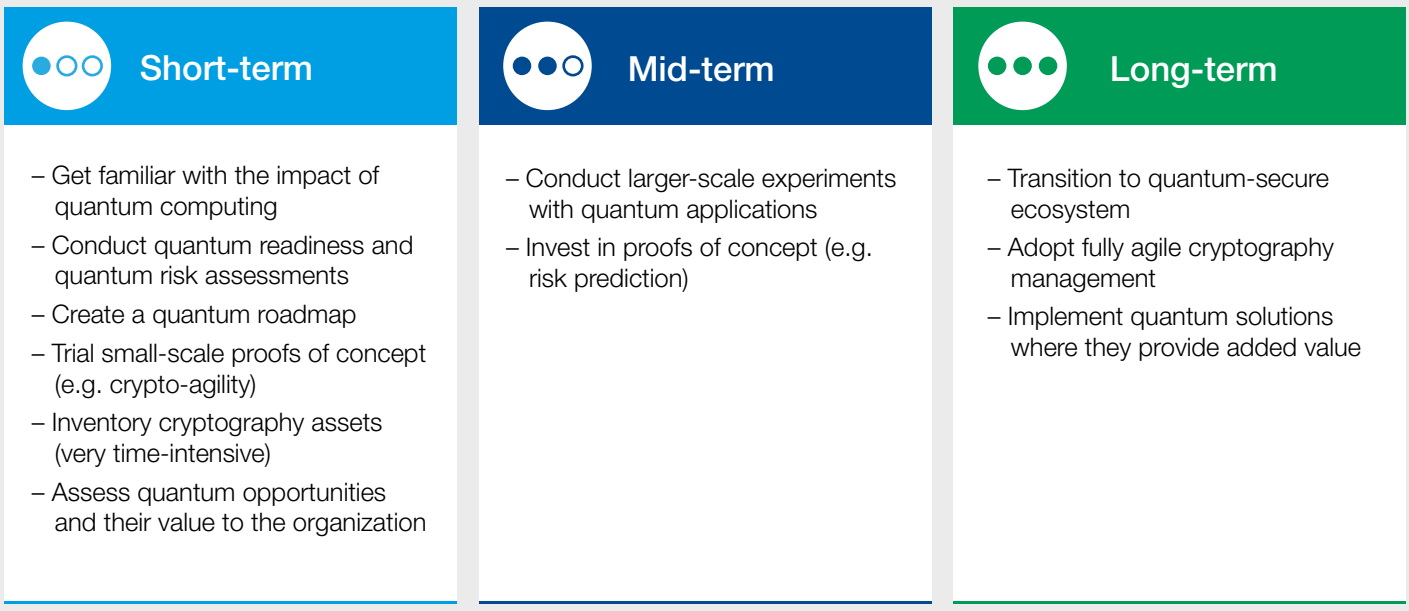
BOX 1 **Understanding the steps to take on quantum: Salesforce**

Like several organizations, Salesforce is currently making the quantum-secure transition. To understand the potential impact and to define an action plan, the first step involves a comprehensive audit of all cryptographic assets. At the same time, Salesforce is tracking public-key standards from NIST and collaborating with potential partners to build internal tools to address and mitigate the quantum threat. These steps allow Salesforce to experiment with different potential public-key standards and determine their impact on the environment, while implementing new tools.

2.2 What can organizations start to do?

Organizations can start assessing the impacts that quantum risk might have on their operations before the quantum threat actually reaches them. They can set short-, medium- and long-term goals today to manage the risk and ensure a smooth quantum transition (see Figure 4).

FIGURE 4 **Goals to manage quantum risk and ensure a smooth transition**



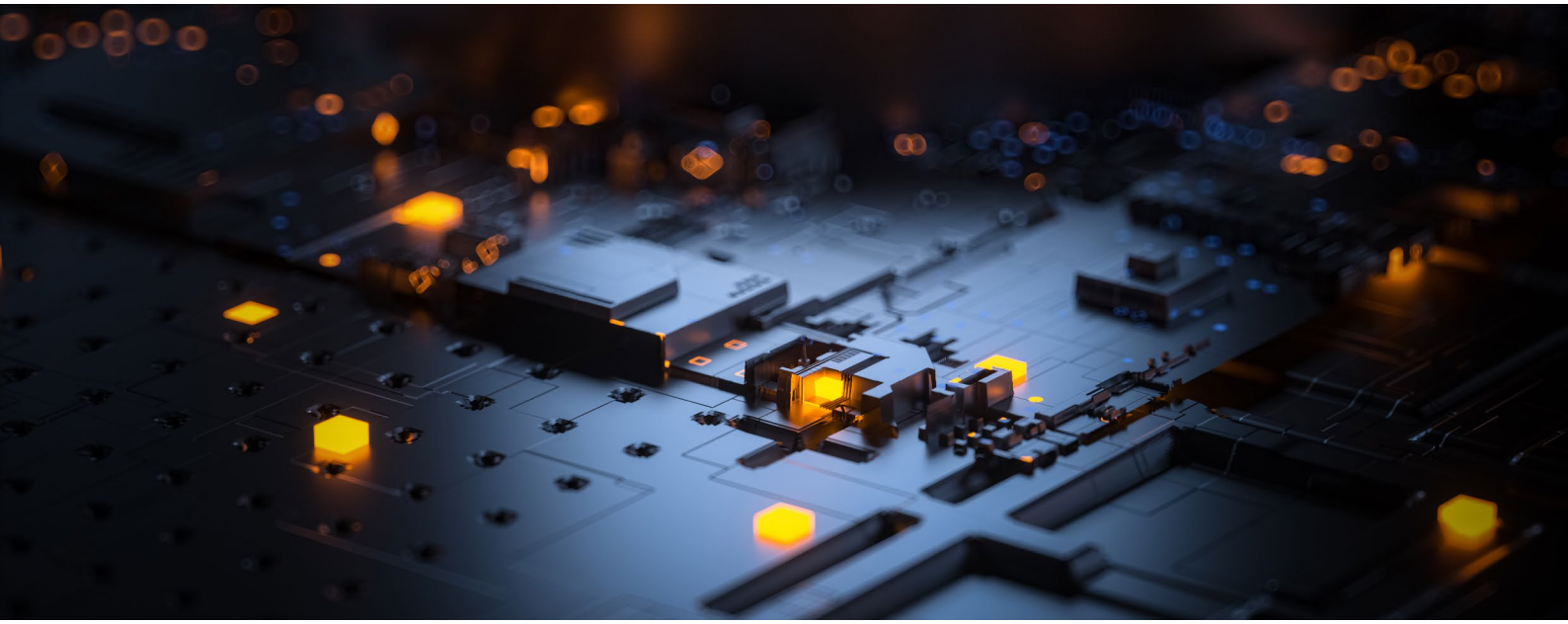
Source: World Economic Forum

BOX 2 | **Partnering on developing quantum proof of concepts: Quantinuum and Fujitsu**

As part of their vision to be ready for quantum risks to network security, Fujitsu partnered with Quantinuum on a software-defined wide area network (SD-WAN) proof of concept (PoC) which incorporated cryptographic keys that would remain secure and unpredictable, even as powerful quantum computers are developed in the future.

The project focused on integrating Quantinuum's key generation platform into Fujitsu's SD-WAN PoC infrastructure. The key generation platform uses quantum computers to generate probably near-perfect cryptographic keys using a verified and patented quantum process. Keys are delivered securely to the SD-WAN nodes and used to encrypt network traffic. Over time, this integration will incorporate post-quantum algorithms, as these become approved by NIST and standardized.

The combination of new, approved algorithms and the PoC approach for their configuration, integration and security benefits on cloud will provide enhanced SD-WAN security and benefits for cloud-hosted application solutions. The technical goal of deploying the solution is a reduction in the potential for data breaches, should the quantum risks to cryptography be realized, thanks to the strong guarantee of cryptographic key strength.



2.3 What are the deployment scenarios?

Hybrid and/or phased approaches to the quantum transition offer the best balance for most companies between potential impacts and opportunities.

There is often a debate on when is the right time to deploy emerging technologies – is it best to be an early adopter of proprietary technology, to wait for consensus standards to evolve, to rely upon the use of frameworks that provide guidance on how to leverage standards, or to wait until regulators force change?

In the case of quantum, underlying standards have been under development by NIST since 2017. NIST announced the initial "winners" in July 2022,[16] which will now be developed into Federal Information Processing Standards (FIPS). Some organizations will rely upon this directly, much as they do with FIPS 140-2 and related examples of this type of document. Other organizations may seek to wait until NIST has offered up the material for an international standard under the International Organization for Standardization (ISO) or the Internet Engineering Task Force (IETF).

National cybersecurity institutions – such as the US's National Security Agency (NSA), the US's Cybersecurity and Infrastructure Security Agency (CISA), the Agence nationale de la sécurité des systèmes d'information (ANSSI – France's computer security service), the Bundesamt für Sicherheit in der Informationstechnik (BSI – Germany's Federal Office for Information Security), Canada's Communications Security Establishment (CSE), and the UK's National Cyber Security Centre (NCSC) – have started to issue implementation guidance and help organizations make decisions on relevant activities.

Nevertheless, some organizations may wait (either deliberately or inadvertently) until they are obliged to act, either by regulation or in response to an actual reported attack on encryption by a quantum computer. Figure 5 presents four potential scenarios for adoption.

FIGURE 5 | **Four potential deployment scenarios to address quantum risk**

Scenario	Rationale	Potential impacts	Potential opportunities
Do nothing	Organizations that believe quantum computing is still at an early stage and the benefits of investing and embarking on the quantum transition are yet to be defined.	– No protection from quantum; full impact on the digital infrastructure – Disruption of business operations and processes – High risk of requiring a reactive, direct changeover when the threat materializes	– No upfront financial outlay
Adopt a hybrid approach	As standards are created, it is possible to have classical, quantum and post-quantum cryptography solutions in a hybrid mode. The security of the complete solution is as good as the strongest element.	– Vulnerability of classical solutions – Low to medium financial impact	– Provides legacy support to old solutions – Allows agility and flexibility to adapt quickly to new solutions – Provides classical protection while PQC algorithms being further stress tested
Follow a phased approach	Phase investment to adopt quantum security solutions to replace impacted solutions.	– Vulnerability of classical solutions – Low to medium financial impact	– Prioritization of solutions based on inventory – Phase-based improvement learnings – Phased budget spending following quantum's evolution
Direct changeover	Make a replacement of all impacted solutions, replacing them with quantum and post-quantum cryptography.	– High financial impact – large migrations can have higher costs – Large disruption of business operations and processes	– Direct enhancement of security against quantum risks for smaller, novel and less complicated environments

Each organization will have to assess its own cost versus impact of quantum risk activities, relative to other priority strategic cyber initiatives, determine which scenario is best and budget accordingly.

BOX 3 | **Running a phased approach at a healthcare provider: QuSecure**

Healthcare data remains relevant for years – and often decades. This puts the healthcare industry at risk of "harvest now, decrypt later" attacks. After learning about the quantum threat, the leadership at a large healthcare provider sought help to start a phased approach to adopting post-quantum cryptographic standards.

A network of clinics within the company has transmitted patient records between physical locations continuously for the past two decades. Given the mix of legacy and modern equipment, any proposed solution should: 1) overlay legacy network infrastructure, 2) support expected network performance and 3) maintain communication with non-upgraded equipment.

To begin the phased approach, a combination of quantum random number generator, post-quantum cryptosystems, protocols and traffic monitoring software was deployed in a single pilot clinic to demonstrate quantum-resilient data transmission. After successful testing, the healthcare provider is now rolling out the solution to a broader number of clinics to ensure a phased and complete transition.

3

How to adopt a quantum risk management approach?

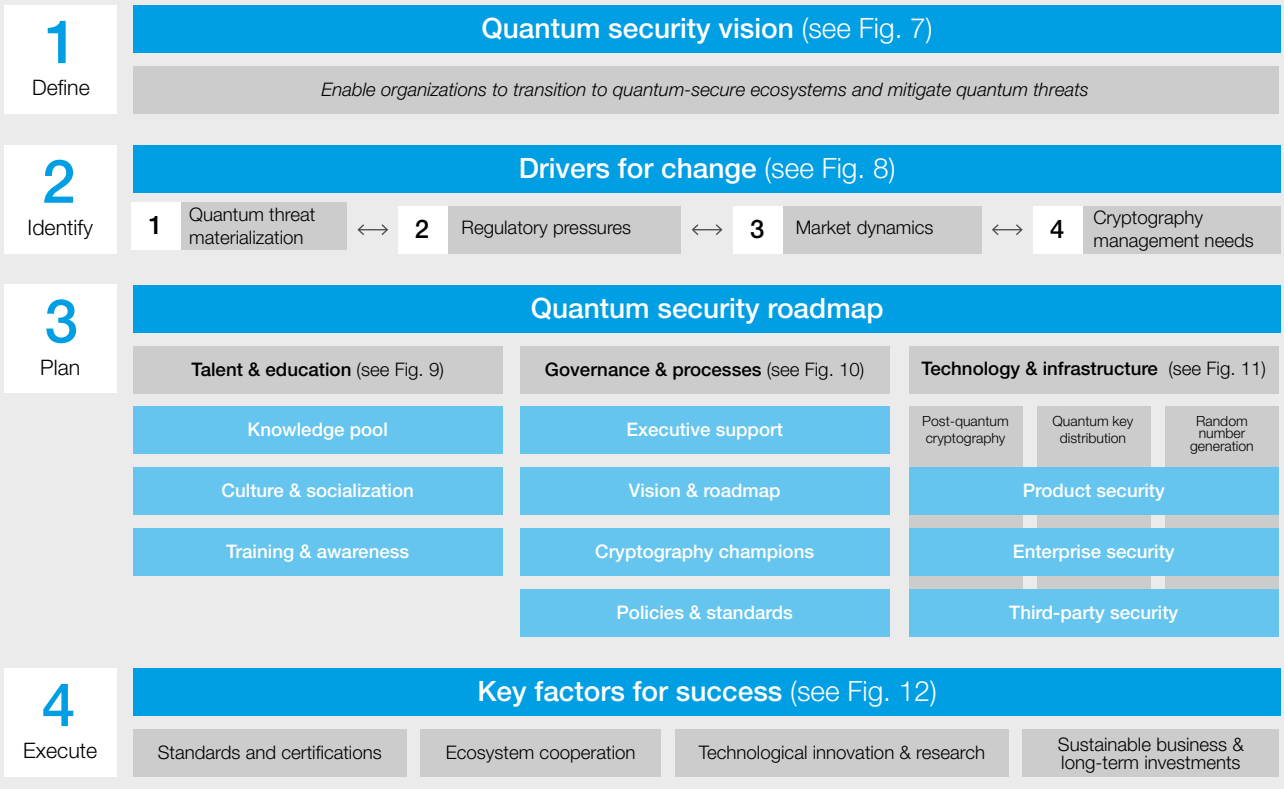
First define your quantum security vision. Identify drivers for change. Then plan and execute your roadmap, while enabling critical success factors.

The World Economic Forum's Quantum-Secure Transition Framework provides guidance for organizations in defining their quantum security transition, by identifying the quantum risks and their timelines against each organization's unique technology environment and digital ecosystem. It is a consensus-based framework developed by the Forum's quantum security community.

The framework consists of four layers – Define, Identify, Plan and Execute – that help organizations structure their goals and objectives for a secure quantum transition (see Figure 6).

> **One way of anticipating the quantum threat timeline could be by considering now which systems need to be left behind**
>
> Brian LaMacchia, Distinguished Engineer, Microsoft Research

FIGURE 6 **Quantum-Secure Transition Framework**



Source: Deloitte, World Economic Forum

3.1 Quantum-Secure Transition Framework

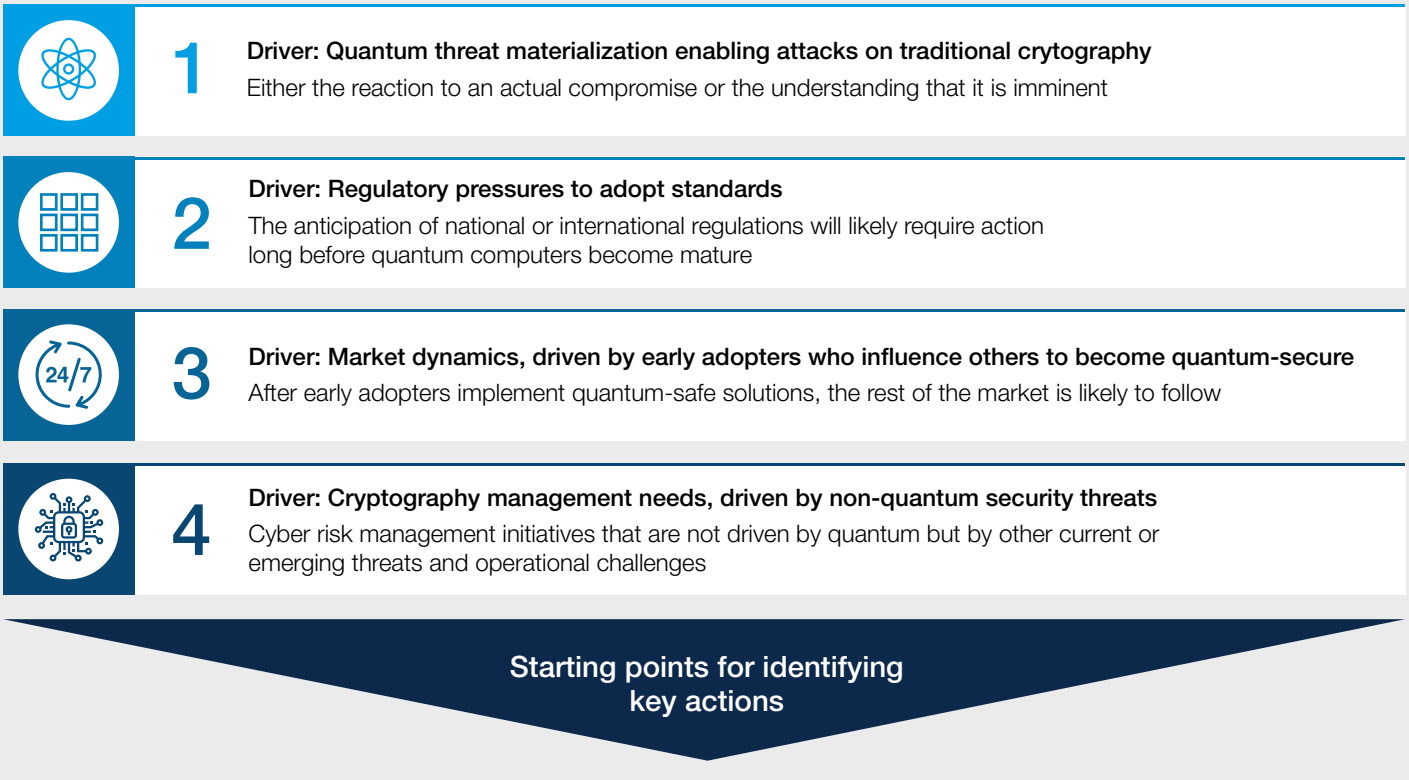
1. Define a quantum security vision
Organizations can define a quantum security vision based on contextual factors, (see Figure 7) including but not limited to organizational strategy, cybersecurity and IT plans, and the market they operate in. Organizations can use their organizational context to create objectives for their quantum transition.

FIGURE 7 **Contextual factors**

Organizational plans	Cybersecurity and IT	External sources
Business strategy Strategic Investment plans	Cybersecurity and IT strategy Cybersecurity and IT politics	Market drivers Regulatory influences

2. Identify drivers for change
There are different drivers that could motivate an organization to kickstart its quantum transition (see Figure 8). These can be threat-driven, but there are also more business-driven reasons for an organization to explore new ways of managing cryptography. The drivers presented in Figure 8 are representative and non-exhaustive. They are independent but possibly interlinked. However, it is still unclear when the impacts of some drivers will materialize, how they will influence each other and how they will influence organizations to change.

FIGURE 8 **Drivers for change**



Source: Deloitte, World Economic Forum

3. Plan a quantum security roadmap
Based on the strategy and drivers, organizations can start defining what actions and approaches need to be prioritized for their own quantum transition. We have identified three workstreams: **Talent & Education, Governance & Processes** and **Technology & Infrastructure**, detailed further in Figures 9, 10 and 11.

FIGURE 9 | **Quantum security roadmap: talent & education**

Knowledge pool
While the materialization of the quantum threat is still several years away, organizations can start equipping their talent with the right knowledge on quantum security. This includes addressing the talent gap.

Culture & socialization
Quantum computers can change the threat landscape for organizations. Socializing this impact can aid the quantum-secure transition.

Training & awareness
Early education and training on quantum and how quantum security impacts the organization provides teams with the ability to be ready when the quantum impact materializes and aids understanding of the threat.

Talent & education: approaches

– Create a realistic timeline now that showcases the time and effort it will take to transition, in order to educate leaders who may believe the threat is too far away to act now

– Lack of understanding around the quantum timeline can be mitigated by demystifying quantum and framing it in relation to the corporate business model

Source: Deloitte, World Economic Forum

FIGURE 10 | **Quantum security roadmap: governance & processes**

Executive support
Projects and transitions revolve around getting proper support from senior leadership to enable appropriate sponsorship, resources and mandate for change.

Vision & roadmap
As becoming quantum-secure becomes a higher priority, initiatives should be bundled and supported with a quantum security roadmap.

Cryptographic champions
Cryptographic champions can look beyond separate functions and amplify the quantum security message at the team level and coordinate adaptation across the organization.

Policies & standards
Successful implementation of policies and standards brings organizations up to speed with regard to new ways of working and reducing the impact of quantum threats.

Governance & processes: approaches

– Integrate the risk of quantum into your general risk management framework to understand the level and likelihood of impact across your ecosystem

Source: Deloitte, World Economic Forum

FIGURE 11 | **Quantum security roadmap: technology & infrastructure**

Post-quantum cryptography
Development and implementation of quantum-safe algorithms that are secure against quantum computer-supported attacks.

Quantum key distribution
Deployment of cryptographic protocols for distribution of symmetric keys, in order to avoid vulnerable key exchange mechanisms.

Random number generation
Generating true random numbers based on the laws of quantum mechanics, as opposed to the pseudo-random numbers generated by traditional techniques.

Product security
Relates to the security of software development or other product design. When conducting product security assessments, teams must take into account the security of the cryptographic protocols in use for their organization's products.

Enterprise security
Helps organizations understand whether they are secure and implementing sufficient measures to safeguard their business and people. Within enterprise security, organizations need to prioritize quantum risk.

Third-party security
Protects an organization against cybersecurity threats that originate from the supply chain, vendors or customers. Assessments may be needed to gain insights into how the quantum threat changes the threat landscape.

Technology & infrastructure: approaches

– To overcome a heavy dependency on vendors and their solutions, organizations can begin to have conversations with vendors about the quantum threat to gain realistic expectations

– To tackle budgetary restrictions, piloting use cases can demonstrate the opportunities that quantum can bring to your business

Source: Deloitte, World Economic Forum

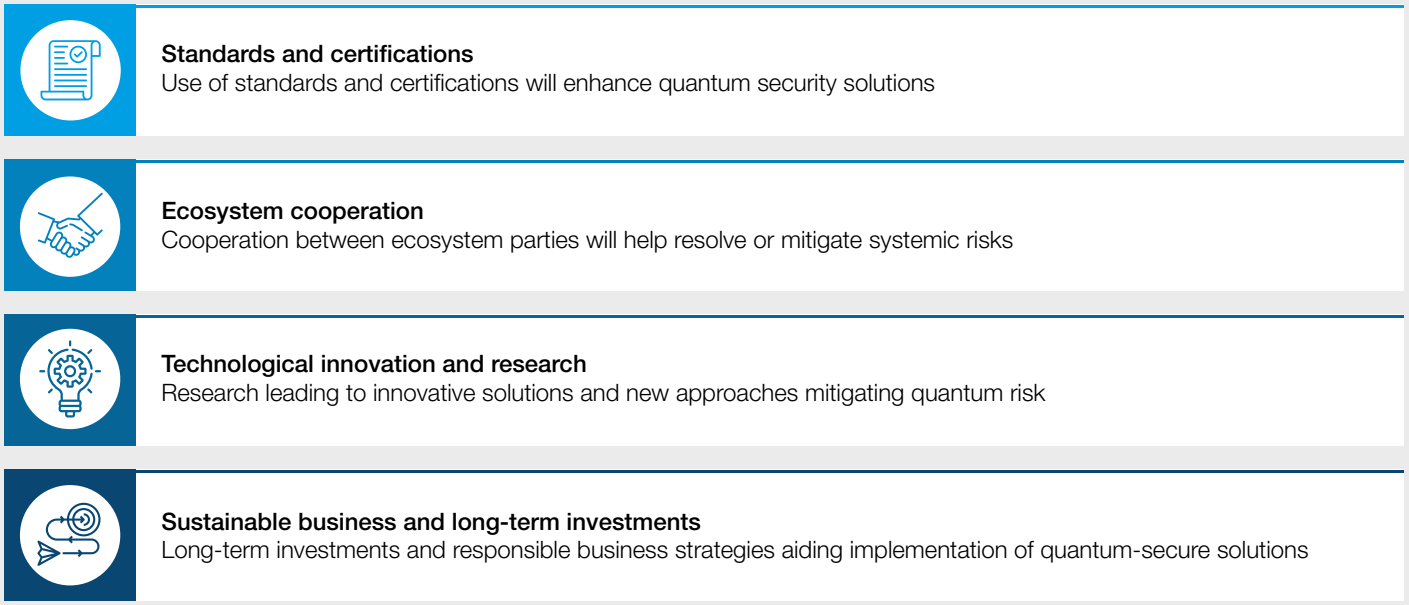
BOX 4 | **Experimenting with specific applications: Banco Santander**

Financial institutions deal with very sensitive data, including customer data and information regarding transactions and contracts. Regulators often require sensitive data to be stored for long periods, making security a key requirement. The advent of quantum threats could therefore have implications on the security of financial institutions. To prepare its enterprise against quantum threats, Banco Santander has been experimenting with a number of strategic research projects, outlined below.

1. Understand the current risks of critical functions handling sensitive information, by mapping the potential threats, and develop a quantum readiness framework for a prioritized transition. This framework helps build a roadmap to developing an understanding of the organization's confidential cloud and digital signature resilience.
2. Identify and assess use cases for random number generation within the bank's services and the benefits of having a quantum-based random number generator solution, such as verifiability and improved performance. These use cases aim to explore novel approaches to improve the overall quality of the bank's random number generation in key areas, including cryptography, financial simulations and machine learning.
3. Initiate implementation of cryptographic agility by developing "cryptography-as-a-service" to provide the bank with the ability to move services over to post-quantum cryptography, as well as the opportunity to make modern cryptographic automation more widely and easily available within the organization.

4. Execute ensuring key factors for success
With an initial roadmap in mind, it is crucial to strategize who should get involved in kickstarting the transition, identifying the key stakeholders and best candidates to get the ball rolling. There are no silver bullets while executing a strategy and plan to address the quantum threat. Organizations will face challenges strategizing which solution is right for them and their specific application, and encounter implementation issues along the way. There are four key factors that will help ensure the successful and robust execution of a quantum security roadmap (see Figure 12).

FIGURE 12 **Key factors for success in executing a quantum security roadmap**



BOX 5 **Developing playbooks for change: EvolutionQ**

The financial services industry is one of the most heavily regulated and relies on trust relationships between customers and financial companies for its survival. The quantum threat puts at risk the backbone of today's financial infrastructure and worldwide economy in the coming years.

To educate multinational investment management and financial services companies on the risk profile and how to ensure a quantum-safe transition, we have conducted detailed analysis on how the risk profile is changing. Risks are increasing with larger and more complex infrastructure, and these risks will only grow with the massive rise in cloud platforms, sophisticated mobile stacks and the advent of edge computing. With that in mind, we have reviewed the key data that could be harvested today and decrypted tomorrow by malicious actors using quantum computers.

We then looked at the benefits of implementing a quantum key distribution (QKD) solution by developing a multi-phase playbook to define requirements for the potential roll-out. This allowed us to establish a two-phase approach that defines a QKD simulator enabling the bank to assess the security and performance potential, followed by the project definition that will replace the simulator with actual QKD hardware.

The solution increases the bank's layered cybersecurity defences by providing the "vault" to lock down the bank's most important assets and prevent the potential risks arising from code-breaking.

4 What is required from different stakeholders?

All organizations will feel the impact of quantum. The transition must begin with leaders setting the right level of support and direction.

Like many other emerging and disruptive technologies, the quantum threat will affect almost everyone. Developing and implementing a successful quantum readiness plan requires coordination across many different industry sectors, governments and global stakeholders. All organizations will feel the impact of the quantum threat, regardless of their size, type and revenue – including quantum technology vendors themselves. The quantum-secure transition must begin with leadership to set the appropriate level of support and direction required to carry out such an effort.

This chapter offers some recommendations for priority activities to the following actors:

- Corporate leaders and boards
- Cyber leaders
- Policy-makers
- Leaders navigating the extended enterprise ecosystem

Smaller organizations or those without a dedicated cyber security office or function could still appoint an officer responsible for quantum reporting to management to ensure the quantum threat receives the right focus and prioritization.

4.1 Recommendations for corporate leaders and boards

Corporate leaders and boards represent the CEO and other C-suite leaders who establish the overall direction and priorities of organizations, including initiatives pertaining to quantum computing technologies.

What you should know

- Understand the capabilities and challenges of adopting quantum technology and the business impact of quantum computing advances.
- Grasp the individual and industry-wide legal and regulatory implications.
- Learn how to navigate the hype and complexity of quantum risk solutions – and properly evaluate the impact on your organization. The Quantum-Secure Transition Framework presented in Chapter 3 of this white paper can help organizations define their vision, objectives and key steps in line with their risk appetite and business drivers.

What you should do today

- Adopt a holistic approach that balances the potential opportunities of quantum computing against the risks. Understand that taking risks may be necessary to fulfil various regulatory and legal responsibilities and that various drivers (regulatory, financial, security etc.) can influence the need for and speed of adoption.
- Invest in updating IT systems and technical infrastructure, and prioritize crypto-agility to avoid lock-in and costly future changes. Consider conducting thorough risk and impact assessments on which solutions (PQC, QKD, QRNG etc.) might suit your organization best.
- Invest in the hiring and training of knowledgeable and skilled staff that understand the technology and the threats. During our interviews and working sessions, most organizations noted that this is the key challenge for the coming years.
- Coordinate quantum security efforts internally, in cooperation with other C-suite stakeholders and risk management functions, to build awareness and integration with supporting and affected corporate functions. Externally, establish third-party risk management functions to include quantum risk preparedness. These third-party stakeholders include key vendors and service providers, channel partners, infrastructure providers, product vendors and other ecosystem partners.

> “The key challenge in the coming years will be hiring staff skilled enough to understand the quantum threat.

4.2 Recommendations for cyber leaders

Cyber leaders represent the chief information security officer (CISO) of the organization, or whoever is the senior-most individual in the organization specifically tasked with protecting its information and technology assets.

What you should know

- Understand the organizations, individuals and entities driving the regulatory and standards conversations (NIST, ENISA, etc.). Chapter 2 of this white paper sheds light on regulatory developments and links these to various scenarios for adopting quantum technologies now and in the future.
- Keep informed of entities advancing in quantum, both security applications and quantum computing threats, through liaising with ecosystem partners, supply chains and other organizations.
- Monitor quantum developments in your organization by working with responsible individuals, such as the owners of crypto infrastructure and cybersecurity, as well as privacy policy teams, data owners and the data protection officer.

What you should do today

- Champion quantum computing concerns within your organization and educate corporate leaders and business stakeholders. Some organizations have successfully created the right level of urgency by linking the quantum threat to operational resilience and business strategies, and tailoring the impact of the quantum threat to the organizational context.
- Launch initiatives to assess quantum computing risks and exposures. Establish or modify processes to account for quantum computing capabilities. Understand that cross-functional collaboration between security, operational and business functions might be critical.
- Build a crypto "inventory" that includes data assets to determine which ones need to be re-encrypted with quantum-resistant cryptographic algorithms. A complete inventory will provide a clear overview of vulnerabilities and which systems might need to be prioritized in the secure quantum transition.

4.3 Recommendations for policy-makers

> Imagine the future of quantum – it is an ever-evolving technology with some exciting opportunities.

Policy-makers represent national and international leadership, along with standards organizations that are ultimately responsible for guiding the governance of quantum technologies and efforts to mitigate their potential risk.

What you should know

- Understand the commercial and national security implications of quantum computing.
- Discern the relationships between different standards to make a timely start in transitioning to quantum-safe standards. We are starting to see guidance from NSA, ANSSI, BSI and others, so keeping track of regulatory movements could be useful in determining what is needed for organizations in your jurisdictions.
- Manage the balance between regulating the technology too early (stifling innovation) and regulating the technology too late. The debate on the right moment to deploy quantum-safe solutions is still ongoing and organizations are looking towards policy-makers and regulators to see when they need to act.

What you should do today

- Support the development of international quantum cybersecurity and risk management standards for quantum computing. A starting point for this can be our Quantum-Secure Transition Framework presented in Chapter 3 of this report.
- Promote enhanced quantum awareness among both public and private sector leaders. Many organizations stress the need for education, especially at a senior level.
- Accelerate development of a cyber-secure global ecosystem by including quantum cybersecurity technology as an area of focus.
- Consider incorporating advances in quantum cybersecurity into existing standards originally written during the classical era.
- Imagine the future of quantum – it is an ever-evolving technology with some exciting opportunities.

4.4 Quantum across the extended enterprise ecosystem

Our modern digital economy is becoming more granular and dispersed, while at the same time increasingly systemic and interdependent. Organizations rely heavily on connected technologies – both custom-developed and off-the-shelf – to execute and maintain their extended and connected supply chains. While organizations may be responsible for legacy, home-grown applications and databases, and their own IoT, mobile devices and internal networks, third-party vendors will most likely manage support technologies, such as public telecommunications, cloud services and common business applications.

When it comes to the quantum transition, organizations should:

- Understand their exposure to potential quantum threats through the lens of their digital supply chain and full partner ecosystem. This includes knowing about core technology solutions and the status of the encryption capabilities within those products.
- Clarify which enterprise technologies and services are the responsibility of the organization itself to make quantum-safe as opposed to those that are the obligation of third parties to address.
- Establish vendor relationships to understand the timelines and expectations around addressing quantum threats in the products and services those vendors provide.

Third-party vendors should be continuously aware of how quantum threats will impact their products and take action to develop enhancements to those products and services. Third-parties should therefore:

- Understand the risk and impact of the quantum threat to their products and services
- Develop a plan to address quantum risks in their product and/or service roadmap
- Communicate their action plan to customers and stakeholders to build awareness and promote action

BOX 6

Creating awareness across the regulatory environment: the UK's Financial Conduct Authority (FCA)

To better understand the potential impacts of quantum information technologies (QIT) on financial services, the FCA has carried out several activities in collaboration with the UK Quantum Computing & Simulation Hub. This is a valuable example of how regulators can collaborate more closely with academia to understand complex technological topics.

In addition to an expert talk and a joint internal report, the FCA co-organized a virtual workshop with more than 25 different stakeholders, including the Bank of England, six leading UK universities, the UK Quantum Communications Hub (QCH), the Engineering and Physical Sciences Research Council (EPSRC), the National Cyber Security Centre (NCSC), the National Quantum Computing Centre (NQCC) and internal stakeholders. The aim of the workshop was to raise awareness of QIT, educate relevant stakeholders in its key potential impacts and identify areas of focus for financial regulators.

The findings from the FCA workshop provided valuable insights around future policy implications and potential regulatory challenges in the areas of security and competition. Similarly, it supported conversations with other international regulators and prompted the sharing of insights across jurisdictions, while gathering novel information about relevant developments.

5

What technologies are available to address the quantum threat?

Quantum computing's threat to public-key encryption has generated a market for quantum risk technologies with varying levels of maturity and relevance to organizations.

In today's nascent quantum cybersecurity market, several efforts are ongoing to develop technologies to mitigate the quantum threat. These technologies do not represent a silver bullet, but they can be used individually or in combination for certain applications. There are three technologies to mitigate the risk posed by quantum to public-key cryptography that have been garnering the majority of attention:

- **Post-quantum cryptography (PQC)** uses new mathematics-based public-key cryptography algorithms that are designed to be impervious to attacks by Shor's algorithm. PQC will fundamentally update what will become insecure cryptographic algorithms.
- **Quantum key distribution (QKD)** develops physics-based quantum techniques to generate secure communication channels which can be used to distribute encryption keys. QKD can complement the use of PQC and other cryptographic algorithms by providing a secure key distribution method.
- **Quantum random number generation (QRNG)** leverages fundamental quantum properties to generate random numbers with high entropy. Randomness is a key part of cryptography. QRNG produces better validated entropic sources than conventional processes, which may enhance security under certain conditions.

> **In the quantum-secure solutions market there is a large information asymmetry between buyers and sellers. Buyers don't always know how to pick the right technical solutions that will mitigate the specific threats their organization faces and sellers are incentivized to sell inferior products based on factors other than solely their technical qualifications. This leads to an adverse selection problem which is a concern for the entire quantum security ecosystem.**
>
> Jaya Baloo, Chief Information Security Officer, AVAST

5.1 Post-quantum cryptograpy

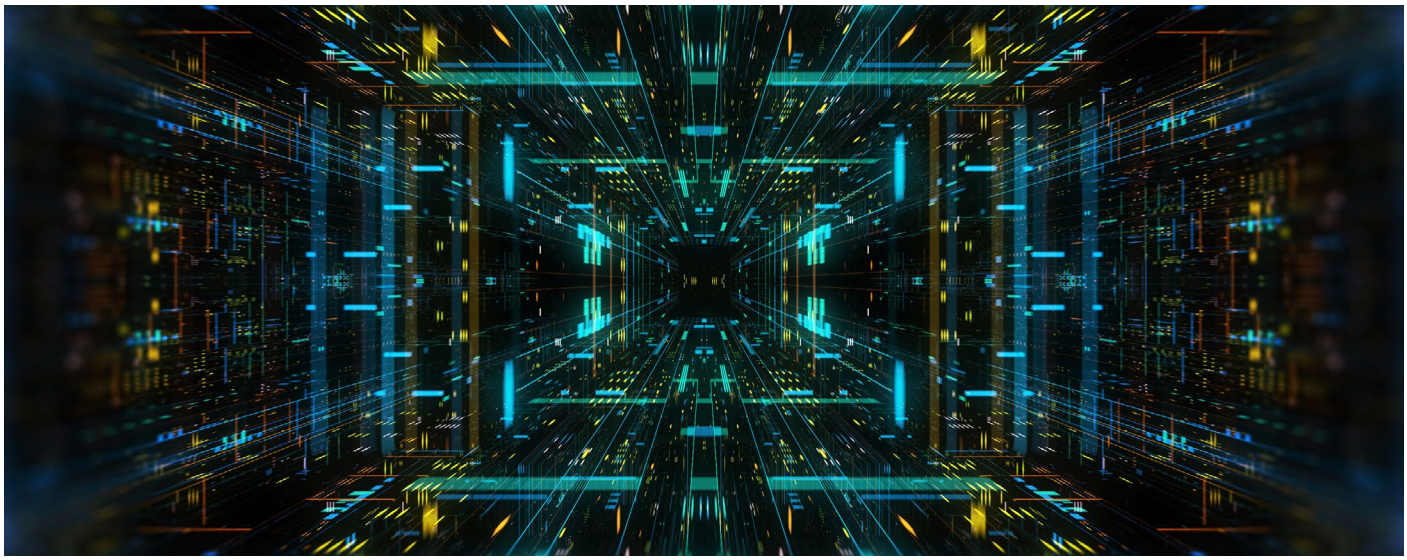
Post-quantum cryptographic algorithms are based on hard mathematical problems, which are very difficult to solve efficiently, even for quantum computers. There are various options and approaches to develop these algorithms with different security levels and use cases. To provide general guidance to where and how to use these algorithms, in late 2017 NIST initiated a process to solicit, evaluate and standardize quantum-resistant public-key cryptographic algorithms. In July 2022, NIST announced a list of four quantum-resistant cryptographic algorithms and is currently developing standards for post-quantum cryptography to protect information exchanges in the quantum era.[20]

Added benefits

- Considered to be secure against (currently known) quantum attacks
- Software-based solutions can be implemented within existing infrastructure

Current limitations

- All known PQC schemes (from the NIST standardization process) have performance drawbacks, such as requiring long keys and long processing times compared to currently used algorithms (e.g. RSA, ECC), which makes them unsuitable as a direct drop-in replacement
- Developments in classical and quantum attacks (cryptoanalysis) might impact the security of these schemes in the future



5.2 Quantum key distribution

Quantum key distribution (QKD) is the most well-known class of quantum protocols to establish a secure communication channel in a way that stealth eavesdropping is not possible. The protocol uses the principle of “superposition” to ensure that an eavesdropper cannot listen in to the communication unnoticed. This protocol is designed to exchange secret keys that are afterwards used to encrypt the communication using quantum-secure symmetric key algorithms, e.g. AES256.

Added benefits

- Information theoretic security, which means that no algorithms can be developed to access the exchanged keys
- Increased protection against harvest-now, decrypt-later attacks, as the key-exchange protocol is not vulnerable to quantum attacks.
- Can be used in combination with other schemes to add a new layer of security

Current limitations

- Significant financial investment as it requires specialized hardware
- Distance limitations until quantum repeaters and/or satellite QKD infrastructure are developed and commercially available; secured and trusted repeaters are needed in the meantime
- Requires a separate authentication channel, which adds additional complexity to the solution, in contrast with current classical methods where authentication is part of the protocol

5.3 Quantum random number generation

Quantum phenomena are inherently random in nature and so can be used to generate pure random numbers. The generation of random numbers plays a crucial role in cryptography, for both the generation of cryptographic keys as well as within some algorithms.

Added benefits

- While classical random number generators (RNGs) are derived from some source of entropy (e.g. thermal noise), QRNGs are inherently random
- The possibility of proof of randomness (certifiable randomness) for some implementations

Current limitations

- Some applications require repeatability, which is not possible for QRNGs
- Difficult to quantify the improvement in security

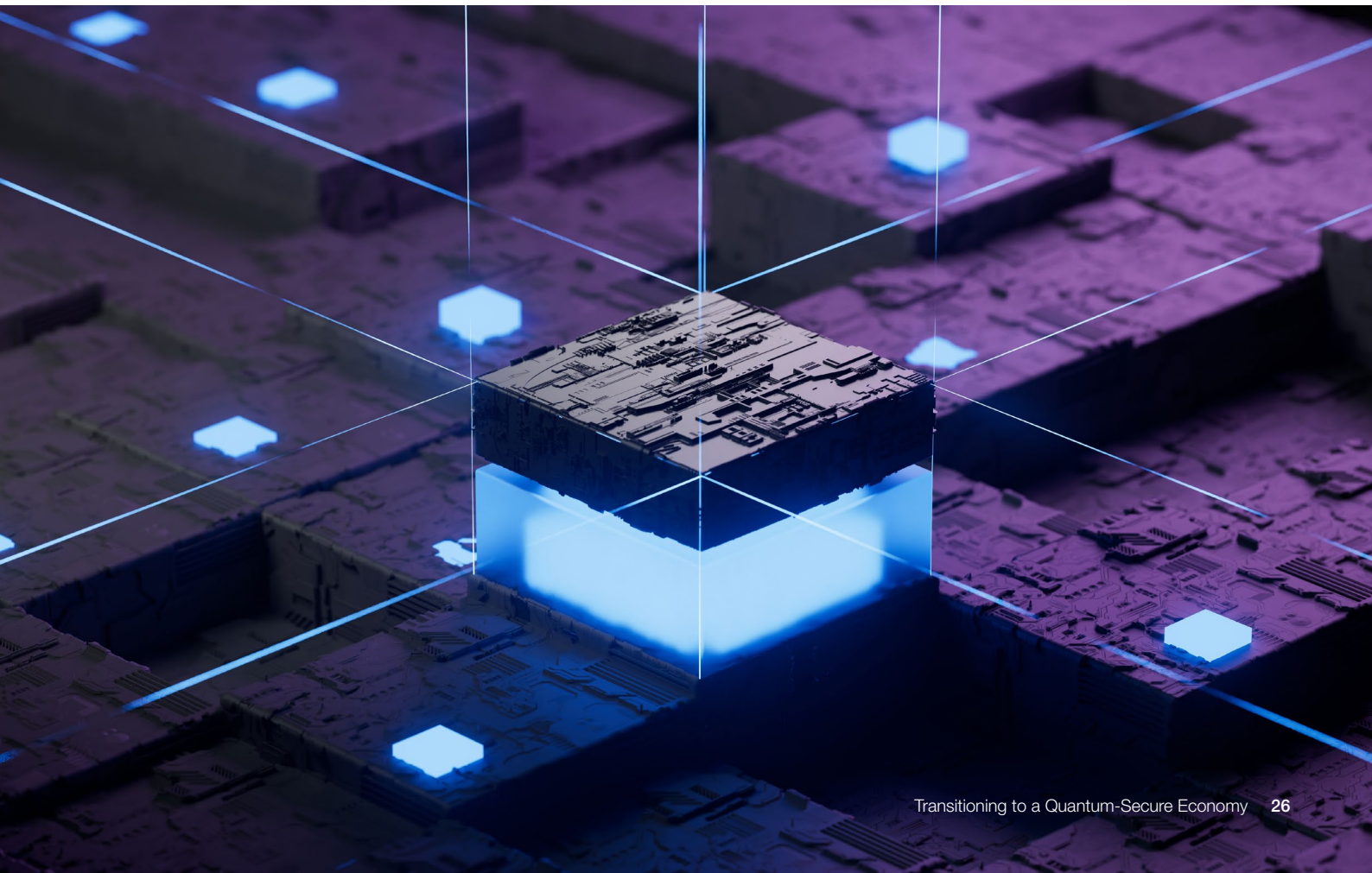
BOX 7

Developing a quantum entropy service for a major global bank: QuintessenceLabs

A major global bank, with an extensive virtual machine deployment hosting a range of banking services, was experiencing delays and the potential for duplicate keys used by the cryptographic processes for securing data and communication. A quantum random number generation (QRNG) solution was explored to ensure the timely delivery of high-quality randomness consumed by the cryptographic processes running in the virtual machines.

The QRNG network appliances were deployed in all of the bank's data centres around the world, delivering entropy-as-a-service. The appliance monitored entropy levels and automatically replenished entropy pools before starvation with quantum random numbers retrieved from the appliances.

Previously, during busy periods, login and cryptographically intensive operations had response delays of several tens of seconds. After the deployment of the QRNG solution, response times improved by up to one hundred times. And while prior to deployment of QRNG, 2.5% of virtual machine instances experienced duplicate keys after start-up, after deployment, no duplicate keys were generated. The solution gave the client clear visibility of demand for randomness across the whole organization.



6 What are the focus areas for future attention?

Quantum computing offers great potential to solve critical problems – but it also presents challenges that will require new technologies and partnerships to tackle.

Quantum computing – still in its early stages with near-term gains in some niche industry use cases – offers great potential to help solve a range of critical problems. This chapter looks ahead to what might happen in the future and explores the challenges that organizations committed to mitigating the quantum threat might face around technology, partnerships and other themes.

> **The protection of the data-centric internet world needs a crypto-agile approach to keep pace with constant innovations starting with the quantum threat and continuing for more flexibility for the future.**
>
> Taher Elgamal, Chief Technology Officer, Salesforce

6.1 Quantum technology predictions

The current state of quantum technology is still nascent, but short- and long-term predictions suggest great potential for a technology that could open new opportunities in the cybersecurity area (see Figure 13).

FIGURE 13 **Quantum technology predictions**

Current state

- Quantum supremacy – proof that a quantum computer can solve some problems better than a classical computer – was demonstrated in 2019 by a team at Google[21]
- In 2021, the largest publicly available quantum computer had 127 qubits, but hardware firms are actively working to increase this number and enable additional uses of the technology[22]
- Initial proofs of concept are being conducted with success in financial services, largely using hybrid systems of quantum and classical computers that split different parts of an algorithm across the two architectures to optimize performance

Short-term prediction

- Noisy, intermediate-scale quantum (NISQ) hardware begins to demonstrate instances of genuine quantum advantage in certain areas of financial services (e.g. capital markets)
- The public and private sectors begin formally rallying behind quantum cryptography, to align on standards and improve encryption techniques
- The use of quantum computing (e.g. quantum machine learning) begins to become a unique differentiator for large institutions; most large cloud providers have a market-ready“quantum-as-a-service” tool

Long-term prediction

- Quantum computing hardware advances to the point where decoherence (a process that causes quantum information to be lost, a significant barrier to today’s quantum computers) can be controlled via quantum error correction and meaningful quantum advantage is solidified
- Modern encryption techniques (e.g. RSA) become easily decrypted by quantum computers; however, most governments, businesses and other large organizations (e.g. those that govern the encryption of the internet) have moved on to quantum-secure forms of encryption (e.g.lattice-based methods)

6.2 Pathways and focus areas for future attention and innovation

Quantum computing brings great potential for businesses and governments to harness, whether to enhance their cyber capabilities or to explore new opportunities. There are four focus areas that require the attention of public and private sector actors:

– Establishing new partnerships

– Innovating through the adoption of emerging technologies

– Preparing for areas of disruption

– Exploring new research opportunities: experimentation as a starting point for growth

Establishing new partnerships

- Kick-start your post-quantum transition today by starting to evaluate your infrastructure and systems using a quantum readiness framework or index that consists of benchmarks across industries, plus guardrails and guidance for exploring the current encryption and algorithm ecosystem. This approach can help organizations identify challenges and bottlenecks associated with specific quantum security risks and risks with post-quantum adoption.
- Create an overarching framework to establish a common language for calibrating risks across business, governments, policy-makers and standard-setters.
- Establish a platform to foster collaboration across industries to partner and align on quantum-secure capabilities and solutions.
- Understand the emerging risks from the interdependencies across organizations' value and supply chains, such as telecommunications, cloud environments, etc. There may be challenges, for example, with the transition from smart technologies (e.g. IoT, OT) to quantum-safe algorithms and unclear timelines around when the quantum threat to those technologies might become tangible.
- Develop a secure supply chain strategy inclusive of software and hardware, so that you can prepare to substitute tech due to any crypto breakthrough, quantum or classical. Plan and start talking to your vendors to ask what their responses are to quantum and begin hardware and software transitions as needed.
- Develop guidelines to create awareness and to provide clear action points to decision-makers for managing a secure quantum transition.

Innovating through the adoption of emerging technologies

- The quantum threat provides an opportunity to proactively review and solve generic and legacy challenges encountered in cryptography management (e.g. certificate management, bad seeds etc.).
- Many organizations see quantum random number generators as key to ensuring sufficient entropy in a post-quantum era.
- At the same time, opinion is divided on whether quantum key distribution would be a requirement for secure communications in future.
- Organizations are not sure whether post-quantum cryptography will mitigate the quantum threat on its own.
- There is a clear desire among participants in the Forum's quantum security community to start experimenting with quantum security solutions.
- Given that the quantum transition might include hybrid solutions (systems with both classical cryptographic and quantum-based encryption components), organizations should enhance their crypto-agility to build ongoing capabilities to evolve cryptographic standards and solutions. This crypto-agile approach requires taking a fresh look at cryptographic governance and exploring novel ways to deploy crypto-agile software frameworks and architectures.

Preparing for areas of disruption

- Market-based and public investment into quantum security solutions testify to the importance of and growing interest in moving towards a post-quantum world, setting the stage for a "first-mover advantage race" between countries.
- Some organizations have expressed doubt around whether harvest-now, decrypt-later attacks are something they should worry about today.
- Decentralized systems running on blockchain require a broad consensus before change can be implemented. This could present a significant challenge in the transition of cryptocurrencies, decentralized finance (DeFi) platforms and Web3 to quantum secure solutions (see Box 8).

BOX 8 **Reviewing the quantum risk to blockchain: Deloitte**

Blockchain technology is disrupting many aspects of our lives, including the use of cryptocurrencies. This technology is enabled by using sophisticated cryptography protocols to replace a central authority with a decentralized governance system.

The use of cryptography within blockchain technology makes it very powerful, but also exposes it to a threat from quantum computers. Recent research[23] shows that a significant portion of cryptocurrencies could be stolen by a malicious actor with a cryptographically relevant quantum computer.

The quantum risk to blockchain presents a number of unique challenges that need to be addressed. For example, the performance of blockchain transactions depends heavily on the performance of the underlying cryptography. Replacing the current algorithms with ones of lower performance could have a detrimental effect on the adoption of blockchain applications. Furthermore, the decentralized nature of blockchain technology requires a broad consensus before change can be adopted. This could result in a very long transition period to post-quantum cryptography – time that we may not have.

It is therefore imperative to start preparing the transition as soon as possible. Not just the selection of new cryptographic algorithms, but also creating the consensus process needed to successfully undergo this transition.

Exploring new research opportunities: experimentation as a starting point for growth

- Organizations require more clarity on how to overcome the information asymmetry between buyers and sellers to make informed decisions on which quantum security solutions fit their organization best.
- Opinions and viewpoints are strongly shaped by roles and background (e.g. the "physicists versus mathematicians and cybersecurity specialists" problem). There is a need for collaboration and interdisciplinary research to overcome stances shaped by backgrounds rather than organizational risk profiles.
- Organizations are encouraged to conduct ongoing assessments to monitor developments in quantum computing, as they relate to both opportunities and threats.
- Organizations should address the talent gap by focusing on training and upskilling the current workforce while working with universities to educate and skill new professionals.

Conclusion

Quantum computing will take time to mature, but that is no excuse to delay preparations. Take prudent action now to start your transition to a quantum-safe future.

“ It is difficult to accurately predict how long it will take before this threat materializes. However, this does not mean that organizations should wait before taking action.

As the quantum era continues to evolve and timelines for technological advancements become clearer, it is important to understand how quantum computers will impact cybersecurity, how they may affect your organization specifically and when the threat could potentially materialize based on your individual enterprise risk profile.

The quantum transition process will be lengthy. Regardless of when we think the threat will materialize, you need to consider what steps need to be taken now and what your organization can do to prepare. Consider creating a transition roadmap to help you define your quantum security vision. To get ready for a secure transition to a quantum-safe economy, organizations should identify key stakeholders, including corporate leaders, board members, cyber leaders, policy-makers and vendors, and assign responsibility accordingly.

The field of quantum computing is still in its infancy and the quantum machines we have today are still far from being able to threaten cybersecurity. It is therefore difficult to accurately predict how long it will take before this threat materializes. However, this does not mean that organizations should wait before taking action. Established businesses, start-ups and researchers are all working on solutions, the most common being post-quantum cryptography (PQC), quantum key distribution (QKD) and quantum random number generation (QRNG).

Each of these solutions helps mitigate different aspects of the quantum threat and each has its own benefits and limitations. Innovation will bring new opportunities and advances in quantum, which can in turn open doors to new partnerships, technologies and research opportunities that can be used to expand current operations.

Contributors

Lead authors

Filipe Beato
Lead, Centre for Cybersecurity, World Economic Forum

Anne Ardon
Junior Manager, Deloitte, Netherlands

Itan Barmes,
Specialist Leader, Deloitte, Netherlands

Chris Knackstedt
Senior Manager, Deloitte, USA

Steering committee

Jaya Baloo
Chief Information Security Officer, Avast Software, Czech Republic

Taher Elgamal
Chief Technology Officer, Security, Salesforce, USA

Isaac Kohn
Partner, Deloitte, Switzerland

Brian LaMacchia
Distinguished Engineer, Microsoft Research, Microsoft, USA

Michele Mosca
Professor, University of Waterloo, Canada

Vikram Sharma
Founder and Chief Executive Officer, QuintessenceLabs, Australia

Colin Soutar
Managing Director, Deloitte, USA

Acknowledgements

This white paper was co-created by many experts and diverse stakeholders in the World Economic Forum's project community on quantum security, as part of the quantum computing network that shared insights and lessons learned, through interviews, design workshops and consultation sessions. The World Economic Forum would like to thank the following individuals for their insightful reviews and feedback.

Andrew Fursman
1QB Information Technologies, Canada

Dimitri van Esch
ABN Amro, Netherlands

Sigmund Kristiansen
Aker BP, Norway

Antia Lamas-Linares
Amazon Web Services, USA

Daniel Cuthbert, Mark Carney
Banco Santander SA, Spain

Dimi Stratakis
Bank of New York Mellon, USA

George Miao
Credit Suisse, Switzerland

Jason Lau, Jacques Francoeur
Crypto.com, Hong Kong SAR

Soon Chia Lim, Jong Chin, Roddy Kok
Cyber Security Agency of Singapore, Singapore

Michael Daniel
Cyber Threat Alliance, USA

Ken Durazzo
Dell Technologies, USA

Christian Cruces Mujica
Deloitte, USA

Marc Verdonk
Deloitte, Netherlands

Bushra AlBlooshi
Dubai Electronic Security Center, United Arab Emirates

Andrew Ward
Emirates Integrated Telecommunications Company PJSC (Du), United Arab Emirates

Pavle Avramović
Financial Conduct Authority (FCA), UK

Haimera Workie
Financial Industry Regulatory Authority (FINRA), USA

Gabriel de Alba
Frontera Energy, Canada

Terril Frantz
Harrisburg University, USA

Bruce Schneier
Harvard Kennedy School of Government, USA

Naveen Kumar Malik
HCL Technologies, UK

Kirk Bresniker
Hewlett Packard Enterprise, USA

Duncan Jones, Nidhi Sharma
Honeywell, UK

Anand Autar
ING Group, Netherlands

James Cemmell
Inmarsat Global, UK

Reena Dayal
Institute of Electrical and Electronics Engineers (IEEE), India

William Dixon
Istari Globalm, UK

Roger A. Grimes
KnowBe4, USA

Tommaso Gagliardoni
Kudelski Security, Switzerland

Hanna Helin
London Stock Exchange Group, UK

John Beric, Paul Trueman
Mastercard, UK

Juhani Eronen
Ministry of Transport and Communications of Finland, Finland

Damien Pang
Monetary Authority of Singapore, Singapore

Roland Fejfar
Morgan Stanley & Co, USA

Carl J. Williams
National Institute of Standards and Technology (NIST), USA

John Stewart, Kevin Hanley
NatWest Group, UK

Hoda Al Khzaimi
New York University Abu Dhabi, UAE

Bryan Ware
LookingGlass Cyber Solutions, USA

Mohammed Zumla
Ofgem, UK

Ali El Kaafarani
PQShield, UK

Rebecca Krauthamer
Quantum Thought, USA

Stacey Jeffery
QuSoft, Netherlands

Ibrahim Almosallam, Sara Alghunaim
Saudi Information Technology Company, Saudi Arabia

Mike Wilkes
SecurityScorecard, USA

Ana Predojevic
Stockholm University, Sweden

Maya Bundt
SwissRe, Switzerland

Bob Blakley
Team8, USA

Rainer Muller
Technische Universität Braunschweig, Germany

Salvador Venegas-Andraca
Tecnologico de Monterrey, Mexico

Marcos Allende Lopez
The Inter-American Development Bank, Japan

Jacob Sherson
University of Aarhus, Denmark

Gabrijela Dreo Rodosek
University of the German Federal Armed Forces (Bundeswehr München), Germany

Mark Barwinski
UBS, Switzerland

Arunima Sarkar, Grigory Shutko
World Economic Forum

The Forum also wishes to acknowledge contributions from Alexey Bocharnikov and Piers Clinton-Tarestad from EY, as well as Scott Alexander and David Shiu from Arqit.

Glossary

The table below provides definitions of the most-used terms throughout this document for reference.

AES	The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. AES256 represents the 256-bit version, while AES128 the 128-bit version.
ANSSI	Agence nationale de la sécurité des systèmes d'information – the government agency responsible for cybersecurity issues in France.
BSI	Bundesamt für Sicherheit in der Informationstechnik (BSI) – the German Federal Office for Information Security
Crypto-agile	The ability of a system to be able to rapidly switch between cryptographic algorithms, cryptographic primitives and other encryption mechanisms without the rest of the system's infrastructure being significantly affected by these changes.
Cryptographically relevant quantum computer	Quantum computers that are capable of actually attacking real-world cryptographic systems that would be unfeasible to attack with a normal computer.
CSE	Communications Security Establishment – Canada's national cryptology agency.
ENISA	The European Union Agency for Cybersecurity – an agency of the EU.
Entanglement	A quantum mechanical phenomenon in which the quantum states of two or more objects have to be described with reference to each other, even though the individual objects may be spatially separated.
FIPS	Federal Information Processing Standard (FIPS) documents define rules, regulations and standards for many aspects of the handling of information by computers and people. They apply to all United States government employees and personnel, including members of the armed forces.
Information theoretic security	A cryptosystem is considered to have information-theoretic security if the system is secure against adversaries with unlimited computing resources and time.
NCSC	The National Cyber Security Centre of the United Kingdom.
NSA	The National Security Agency is a national-level intelligence agency of the United States Department of Defense, under the authority of the Director of National Intelligence.
Quantum supremacy	The demonstration of a quantum computer that can carry out tasks that are not possible or practical with a traditional (classical) computer.
RSA	A public-key algorithm that is used for key establishment and the generation and verification of digital signatures.
Superposition	The ability of a quantum system to be in multiple states at the same time until it is measured.
Y2Q	Year to Quantum, the moment when quantum computers can mount attacks on current cryptography.

Endnotes

1. "Overview on quantum initiatives worldwide – update mid-2021", *Qureca*, 19 July 2021, https://qureca.com/overview-on-quantum-initiatives-worldwide-update-mid-2021/.
2. Temkin, Marina, "Investors bet on the technologically unproven field of quantum computing", *PitchBook*, 13 September 2021, https://pitchbook.com/news/articles/quantum-computing-venture-capital-funding.
3. "Quantum Security Market Expected to Reach Over $3 Billion by Middle of Decade", *The Quantum Insider*, 10 November 2021, https://thequantuminsider.com/2021/11/10/quantum-security-market-expected-to-reach-over-3-billion-by-middle-of-decade/.
4. Tett, Gillian, "Encryptogeddon is coming for us all", *FT Magazine*, 1 June 2022, https://www.ft.com/content/a8204a7d-2922-4944-bdff-5449a8f3aee9.
5. Arute, Frank et al., "Quantum supremacy using a programmable superconducting processor", *Nature,* 23 October 2019, https://www.nature.com/articles/s41586-019-1666-5.
6. Lavoie, Jonathan and Zachary Vernon, "Beating classical computers with Borealis", *Xanadu*, 1 June 2022, https://www.xanadu.ai/blog/beating-classical-computers-with-Borealis.
7. Swayne, Matt, "China's Quantum Supercomputer Sets Quantum Supremacy", *The Quantum Insider*, 30 June 2021, https://thequantuminsider.com/2021/06/30/chinas-superconducting-quantum-computer-sets-quantum-supremacy-milestone/.
8. "Executive Order on Enhancing the National Quantum Initiative Advisory Committee", *The White House, US Government*, 4 May 2022, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/05/04/executive-order-on-enhancing-the-national-quantum-initiative-advisory-committee/.
9. "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems", *The White House, US Government*, 4 May 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/.
10. World Economic Forum, *Quantum Computing Governance Principles*, January 2022, https://www3.weforum.org/docs/WEF_Quantum_Computing_2022.pdf.
11. "Global Future Council on Cybersecurity", *World Economic Forum*, 2022: https://www.weforum.org/communities/gfc-on-cybersecurity.
12. Mosca, Michele and Marco Piani, *Quantum Threat Timeline Report 2021*, Global Risk Institute, January 2022, https://globalriskinstitute.org/publications/2021-quantum-threat-timeline-report/.
13. Mosca, Michele, "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?," in *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38-41, September/October 2018, doi: 10.1109/MSP.2018.3761723.
14. Gidney, Craig and Martin Ekera, "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits", *Quantum 5,* 433 (2021), 15 April 2021, https://quantum-journal.org/papers/q-2021-04-15-433/.
15. Webber, Mark et al., "The impact of hardware specifications on reaching quantum advantage in the fault tolerant regime", *AVS Quantum Science*, 25 January 2022, https://avs.scitation.org/doi/10.1116/5.0073075.
16. "Post-Quantum Cryptography", *NIST*, July 2022, https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/evaluation-criteria/security-(evaluation-criteria).
17. World Economic Forum, *Global Cybersecurity Outlook 2022*, January 2022, https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf.
18. "Quantum computers and the Bitcoin blockchain", *Deloitte*, https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/quantum-computers-and-the-bitcoin-blockchain.html.
19. World Economic Forum, *Global Future Council on Quantum Computing: Frequently Asked Questions*, June 2020, https://www3.weforum.org/docs/WEF_Global_Future_Council_on_Quantum_Computing.pdf.
20. "NIST Announces First Four Quantum-Resistant Cryptographic Algorithms", *NIST*, 5 July 2022, https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms.
21. Arute, Frank et al., "Quantum supremacy using a programmable superconducting processor", *Nature*, 23 October 2019, https://www.nature.com/articles/s41586-019-1666-5.
22. "IBM Unveils Breakthrough 127-Qubit Quantum Processor", *IBM Newsroom*, 16 November 2021, https://newsroom.ibm.com/2021-11-16-IBM-Unveils-Breakthrough-127-Qubit-Quantum-Processor.
23. "Quantum computers and the Bitcoin blockchain", *Deloitte*, https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/quantum-computers-and-the-bitcoin-blockchain.html.

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org